Kentucky Wesleyan College
Policy & Procedure Manual

Records Retention[1]

Approval: President

Policy Type: College

Policy Owner: Vice President for Academic Affairs

Responsible Office: Vice President for Academic Affairs

Revision History

Approval Date: March 2013

Modified:

Next Review: May 2016

---

1. **Purpose**

1.1. This policy addresses the retention and disposal of Kentucky Wesleyan College's documents and records as defined below. The College is responsible for retaining paper and electronic documents in a safe and secure environment to ensure confidentiality, security, and archiving as well as proper document destruction once documents have served their purpose. This policy turns intentional document destruction into a process that must be carefully monitored. This policy is designed to eliminate accidental or innocent document destruction. In addition, it is important for personnel to know the length of time records should be retained to be in compliance. An effective document retention and destruction policy reduces the search, retrieval, and production costs of discovery when stored documents must be produced.

2. **Scope**

2.1. No one person or unit can be responsible for all college documents. Therefore every office managing College documents or records is responsible for:

- Implementing documents and records management practices consistent with this Policy
- Educating staff in the documents and records management practices.
- Preserving documents and records as required under this Policy

[1] *Adapted from Fordham University Records Retention and Disposal Policy, Hamilton College Records Retention Policy, and the National Council of Non-Profits sample policies from The Public Council Law Center and the American Institute for Certified Public Accountants.*

- Properly disposing of inactive documents and records at the end of the applicable retention period.
- Protecting documents and records against misuse, misplacement, damage, destruction, or theft.
- Monitoring compliance with this Policy.

2.2. This policy is written with considerations for compliance with federal mandates and acts including The Sarbanes-Oxley Act, Health Insurance Portability and Accountability Act (HIPPA), The Fair Credit and Accurate Transaction Act (FACTA), Gramm-Leach-Bliley (GLB) and other federal, state and local mandates.

3. **Definitions**

3.1. Types of College Records

3.1.1. Record

3.1.1.1. An **Active Record** is any document or record that is currently in active use by an office or function of the College.

3.1.1.2. An **Archival Record** is an inactive document or record that has permanent or historic value and is not required to be retained in the office in which it was originally generated. Archival Records are retained in the College Archives.

3.1.1.3. An **Electronic Record** is a document or record kept in an electronic format, such as a word processing document, a spreadsheet, a database, a scanned or imaged document, and any other type of file stored on a computer, server or mainframe storage device or medium, or on any external or offsite storage medium, or with a third party acting as the College's agent. Electronic Records have the same retention periods as paper and other tangible Records.

3.1.1.4. An **Inactive Record** is a document or record that is no longer an Active Record but still must be maintained pursuant to the Records Retention Schedule set forth below. Inactive Records are typically maintained in specified locations on campus such as the business office, development office or at an off-campus storage site; however, Inactive Records of historical significance are maintained in the College's Archives.

3.1.1.5. A Record with **Personal Information** is a document or record that includes an individual's name or personal mark together with that individual's social security number; driver's license number or other government identification card number; financial account number, credit or debit card number, or any number or code which may be used alone or in conjunction with another piece of information to assume the identity of another person, access financial resources, or obtain credit information. Personal Information is highly sensitive and must be safeguarded and secured at all times.

4. **Policy**

4.1. College documents and records are the property of the College and not the officers, faculty members or employees who create them or to those with whom they are entrusted.

4.2. Administration

4.2.1. **Responsibilities of the President**. The President shall be the administrator in charge of this Policy and has the ultimate responsibility for ensuring the College complies with this Policy. However, since no one person can be responsible for all college documents, each Vice President or Senior Administrator of an area not overseen by a Vice President, is responsible for ensuring their respective areas are in compliance with this policy so that the College may meet its operational and legal obligations and preserve its historical record. The President may modify the Document/Records Retention Schedule from time to time as necessary to comply with law and/or to include additional or revised document categories as may be appropriate to reflect College policies and procedures. The President is authorized to periodically review this Policy and Policy compliance with legal counsel and to report to the Trustees as to compliance.

4.2.2. **Responsibilities of Trustees, Faculty, Staff, and Outsiders.** This Policy also relates to the responsibilities of Trustees, staff, and outsiders with respect to maintaining and documenting the storage and destruction of the College's documents and/or records. It is the responsibility of every employee to comply with this policy. It is the responsibility of any individual who supervisors, manages, or directs a department or function to ensure their employees are aware of the policy and adhere to it. Outsiders may include vendors or other service providers. Depending upon the sensitivity of the documents and/or records involved with the particular outsider relationship, the College, through the appropriate Vice President or Senior Administrator of an area not overseen by a Vice President, shall share this Policy with the outsider, requesting compliance. In particular instances, the College may require that the contract with the outsider specify the particular responsibilities of the outsider with respect to this Policy.

4.3. Suspension of Document and/or Records Destruction - Compliance.

4.3.1. The College becomes subject to a duty to preserve (or halt the destruction of) documents and/or records once litigation, an audit or a government investigation is reasonably anticipated. Further, federal law imposes criminal liability (with fines and/or imprisonment for not more than 20 years) upon whomever "knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States … or in relation to or contemplation of any such matter or case." Therefore, if the President, any Trustee or employee becomes aware that litigation, a governmental audit or a government investigation has been instituted, or is reasonably

anticipated or contemplated, he/she shall immediately notify the President who will order a halt to all document destruction under this Policy, communicating the order to all affected constituencies in writing. The President may thereafter amend or rescind the order only after conferring with legal counsel. Failure to comply with this Policy, including, particularly, disobeying any destruction halt order, could result in possible civil or criminal sanctions. In addition, for employees, it could lead to disciplinary action including possible termination.

4.4. Electronic Documents and/or records – Document/Record Integrity.

4.4.1. Documents and/or records in electronic format shall be maintained just as hard copy or paper documents are, in accordance with the Documents/Records Retention Schedule. Due to the fact that the integrity of electronic documents, whether with respect to the ease of alteration or deletion, or otherwise, may come into question, the Administrator shall attempt to establish standards for document integrity, including guidelines for handling electronic files, backup procedures, archiving of documents, and regular checkups of the reliability of the system; provided, that such standards shall only be implemented to the extent that they are reasonably attainable considering the resources and other priorities of the organization.

4.5. Privacy

4.5.1. It shall be the responsibility of the President, after consultation with counsel, to determine how privacy laws will apply to the organization's documents and/or records from and with respect to employees and other constituencies; to establish reasonable procedures for compliance with such privacy laws; and to allow for their audit and review on a regular basis.

4.6. Emergency Planning

4.6.1. Documents and/or records shall be stored in a safe and accessible manner. Documents which are necessary for the continued operation of the organization in the case of an emergency shall be regularly duplicated or backed up and maintained in an off-site location. The President shall authorize the development of reasonable procedures for document retention in the case of an emergency.

4.7. Document Creation and Generation

4.7.1. The President, Vice Presidents, or Senior Administrator of an area not overseen by a Vice President shall discuss with staff the ways in which documents are created or generated. With respect to each employee or organizational function, an attempt to determine how best to create documents so they can be easily segregated from others, so that, when it comes time to destroy (or retain) those documents, they can be easily culled from the others for disposition. For example, on an employee-by-employee basis, are e-mails and other documents of a significantly non-sensitive nature so that they might be deleted, even

in the face of a litigation hold with respect to other, more sensitive, documents? This dialogue may help in achieving a major purpose of the Policy -- to conserve resources -- by identifying document streams in a way that will allow the Policy to routinely provide for destruction of documents. Ideally, the organization will create and archive documents in a way that can readily identify and destroy documents with similar expirations.

4.8. Document/Records Retention Schedule

4.8.1. Documents should be retained according to the attached Records Retention Schedule. Each office that generates official records must develop, update, and adhere to the official retention schedule pertinent to the responsibilities carried out in that office. These schedules include:

- Description of Official Record
- Recommended minimal retention period (Note that guidance on retention times for many types of official records are provided by law and/or professional associations.)
- Retention period at Kentucky Wesleyan (which may be longer than mandated by law)
- Where records are maintained
- Method of disposal or records transfer
- Departmental responsibility for maintenance and destruction of records
- Whether these records are confidential, and, if not restricted under FERPA, how long the restriction should last.
- Whether these records should be transferred to the College Archives at the end of the retention period

4.8.2. In summary, records may only be destroyed if all retention periods have expired, all audit requirements have been satisfied, there are no pending requests for information, and there is no foreseeable litigation involving the records. All customer complaint documents should be maintained until a finite conclusion has been made.

4.9. Disposal

4.9.1. Disposal of records which have been maintained pursuant to this Policy and which need not be archived or kept should be destroyed. The College and Kentucky law requires that any sensitive or identifying personal information existing in such records (such as social security number, driver's license number, mother's maiden name, account number or code, or personal financial information) be disposed of in a manner that will prevent unauthorized individuals from accessing the information.

4.10. Responsibility

4.10.1. It is the responsibility of every employee to comply with this policy.

4.10.2. It is the responsibility of any individual who supervisors, manages, or directs a department or function to ensure their employees are aware of the policy and adhere to it.

4.10.3. It is the responsibility of each Vice President or Senior Administrator of an area not overseen by a Vice President, to ensure their respective areas are in compliance with this policy so that the College may meet its operational and legal obligations and preserve its historical record.

_____